

JACKIE SPEIER
14TH DISTRICT, CALIFORNIA

2465 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0514
(202) 225-3531
FAX: (202) 226-4183

155 BOVET ROAD, SUITE 780
SAN MATEO, CA 94402
(650) 342-0300
FAX: (650) 375-8270

WWW.SPEIER.HOUSE.GOV
WWW.FACEBOOK.COM/JACKIESPEIER
WWW.TWITTER.COM/REPSPEIER

Congress of the United States
House of Representatives
Washington, DC 20515-0514

December 15, 2015

COMMITTEE ON ARMED SERVICES

SUBCOMMITTEES:
RANKING MEMBER, OVERSIGHT AND
INVESTIGATION
MILITARY PERSONNEL

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE

SUBCOMMITTEES:
EMERGING THREATS
NSA AND CYBERSECURITY

Senior Whip

The Honorable Ashton Carter
Secretary of Defense
1400 Defense Pentagon
Washington, DC 20301-1400

Secretary Carter:

As members of Congress, we write to express serious concern about the decreasing retention of, and rapidly rising need for, certified cybersecurity Red Team testing personnel at the Department of Defense (DOD). As the number and severity of the cyberthreats against the United States continues to mount, realistic cybertesting must become a critical priority that cannot be accomplished without adequate and skilled personnel to do the testing. We strongly urge you adopt enhanced measures to attract, train, and retain such personnel.

In recent months, there have been serious cyberattacks and cyber-intrusions detected in numerous U.S. Government networks, including the network used by the Joint Staff. Such cyberattacks could result in significant damage to the weapons systems and information networks that we rely on for our national security. Both you and the Chairman of the Joint Chiefs of Staff have directed that military services and combatant commands include cyberattacks as part of their training exercises, to confirm that our military can fight through cyberattacks. And last year, the director of Operational Test and Evaluation issued policy that requires more realistic cybersecurity assessments for systems to be fielded to our military.

These goals can only be accomplished if adequate funding and personnel are available for the DOD Red Teams to conduct realistic cybersecurity testing. In order to eliminate security flaws in weapons systems and information networks, we rely on certified cyber Red Teams to conduct realistic cyberattacks during exercises and cybersecurity assessments. Combatant commanders, military service acquisition authorities, and operational testers all require expert support from elements of these cyber Red Teams in order to conduct realistic cyberattacks during training exercises and system testing. The Department needs these Red Teams to portray an array of cyber adversaries, including advanced, persistent cyberthreats from nation-states.

We understand that the number of events requiring cyber Red Team support has more than doubled in the last several years, and Department experts project the Red Team demand will more than double again over the next five years. Furthermore, we understand that in the past year, numerous senior Red Team members have left DOD positions for more lucrative positions in the private sector. The increasing Red Team demand, coupled with the decreasing number of

experienced personnel, indicates that DOD may soon face a severe shortage of qualified cyber Red Team personnel. Such a shortage would significantly hamper the Department's ability to prepare for cyberattacks.

In order to attract and retain the required number of expert cyber Red Team personnel, we strongly urge DOD to consider innovative compensation approaches such as those used in other key specialty areas. It is critical that we not only maintain the ranks and expertise of existing DOD cyber Red Team personnel, but that we make significant investments in their capabilities, training, and retention.

In addition to innovative compensation, Red Teams should be manned, trained, and equipped with sufficient well-qualified personnel to meet the anticipated demand. Red Teams need the tools and skills to emulate a nation-state adversary, they need certification standards to ensure proper manning at journeyman and master levels, and a comprehensive retention plan to ensure a stable workforce.

We request that you outline the steps you plan to take to ensure the Department's cyber Red Teams will be manned, trained, and equipped with sufficient well-qualified personnel to meet the anticipated demand. Please include in your response any proposed changes to current legislation you believe would help you acquire and retain well-qualified cyber Red Team personnel.

Thank you for your attention to this matter, and we look forward to your response.

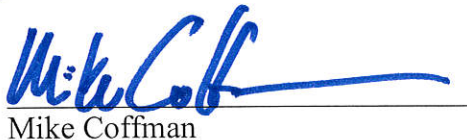
Sincerely,



Jackie Speier



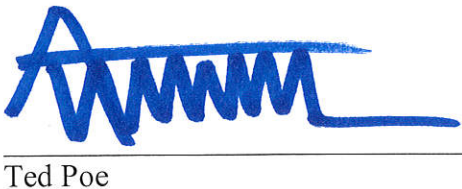
Adam Schiff



Mike Coffman



Walter B. Jones



Ted Poe



Steve Israel


Mike Quigley


Jan Schakowsky

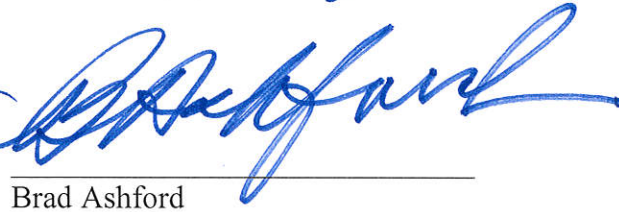

Anna G. Eshoo


Joaquin Castro


Mike Thompson


Patrick Murphy

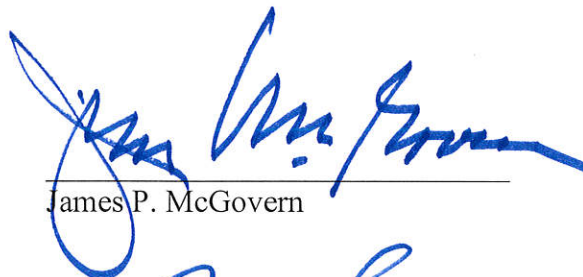

David Schweikert

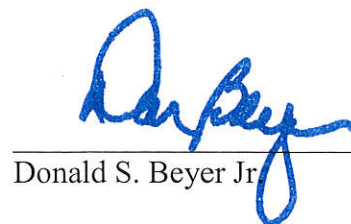

Brad Ashford


Ted W. Lieu


Chris Stewart


William R. Keating


James P. McGovern



Donald S. Beyer Jr


Zoe Lofgren


Tony Cárdenas


Michael M. Honda


Chris Van Hollen


James A. Himes


Cheri Bustos


Kyrsten Sinema